(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
24 juin 2004 (24.06.2004)

PCT

(10) Numéro de publication internationale
WO 2004/054198 A2

(51) Classification internationale des brevets[7] : H04L 29/06

(21) Numéro de la demande internationale :
PCT/FR2003/050132

(22) Date de dépôt international :
25 novembre 2003 (25.11.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/15144 2 décembre 2002 (02.12.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **ARKOON NETWORK SECURITY** [FR/FR]; 13, avenue Victor Hugo, F-69160 Tassin la Demi Lune (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **FAGES, Daniel** [FR/FR]; 4, rue de la Gare, F-01700 Neyron (FR). **LAFON, Mathieu** [FR/FR]; 4A, rue de Mailly, F-69300 Caluire (FR). **BRODART, Benoit** [FR/FR]; 8, rue Franklin, F-69002 Lyon (FR).

(74) Mandataires : **GRYNWALD, Albert** etc.; Cabinet Grynwald, 127, rue du Faubourg Poissonnière, F-75009 Paris (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** ACCESS METHOD AND DEVICE FOR SECURING ACCESS TO INFORMATION SYSTEMS

(54) **Titre :** PROCEDE ET DISPOSITIF D'ACCES POUR SECURISER L'ACCES AUX SYSTEMES D'INFORMATION

(57) **Abstract:** The invention relates to an access method and device for securing logical access to computer resources (2) and/or information (1) belonging to a group of computer equipment (3), whereby logical access is slowed down as little possible. The group of computer equipment (3) exchanges data (4) with a computer telecommunication network (5) via said access device (6). The data (4) comprise data which are transported (7) in compliance with at least one application protocol (8) and transport data (9). The access device (6) consists of: an operating system (10) comprising one analysis module (14) which is suitable for each application protocol (8), and filtration means which are used to filter the aforementioned transported data (7) in the operating system (10) using the above-mentioned analysis modules (14).

(57) **Abrégé :** L'invention concerne un procédé et un dispositif d'accès pour sécuriser l'accès logique à des informations (1) et/ou à des ressources informatiques (2) d'un ensemble d'équipements informatiques (3) en ralentissant le moins possible l'accès logique. L'ensemble d'équipements informatiques (3) échange des données (4) avec un réseau de télécommunication informatique (5), via ledit dispositif d'accès (6). Les données (4) comportent des données transportées (7) conformément à au moins un protocole applicatif (8) et des données de transport (9). Le dispositif d'accès (6) comprend - un système d'exploitation (10) comportant un module d'analyse (14) approprié pour chaque protocole applicatif (8), - des moyens de filtration pour filtrer, dans ledit système d'exploitation (10), lesdites données transportées (7), au moyen desdits modules d'analyse (14).

WO 2004/054198 A2

PROCEDE ET DISPOSITIF D'ACCES POUR SECURISER L'ACCES AUX SYSTEMES D'INFORMATION

La présente invention concerne un procédé et un dispositif pour sécuriser l'accès aux systèmes d'information.

Définitions

Au sens de la présente invention, on désigne d'une manière générale par "applications" des applications logicielles dans le domaine des communications.

Au sens de la présente invention, on désigne d'une manière générale par protocole "applicatif" un protocole qui régit l'échange d'information entre applications.

Au sens de la présente invention, on désigne d'une manière générale par attaque applicative une attaque qui utilise :

- soit les vulnérabilités d'un protocole "applicatif",
- soit les vulnérabilités liées à l'implémentation par un développeur d'un protocole "applicatif",
- soit les vulnérabilités liées à l'utilisation d'une application, notamment par un administrateur réseau.

Le problème posé

Contexte : Sécurité d'accès aux systèmes d'information

Tous les experts s'entendent sur le fait que le risque lié à la sécurité informatique est en très forte progression.

Quels sont les facteurs de croissance de ce risque ?

Trois facteurs principaux ont été identifiés.

Premier facteur de risque : la croissance exponentielle du nombre de pirates.

Le nombre des internautes a été multiplié par deux en trois ans. Ils disposent de boîtes à outils en libre-service sur le net. Les législations internationales visant à réduire les fraudes sont inexistantes ; par exemple au Japon il n'y a pas de loi sur la cyber-délinquance. Enfin, on constate un développement d'un nouveau type de pirate dans les lycées et les campus universitaires pour qui le piratage est un jeu et cracker le plus grand nombre de sites un concours. Ces pirates informatiques, communément appelés des "script kiddies" n'ont que peu de connaissances techniques, mais ils utilisent des "boîtes à outils" de programmes, généralement trouvées sur Internet, permettant d'attaquer des systèmes informatiques.

Deuxième facteur de risque : la mondialisation des échanges.

Dans l'ère de l'entreprise communicante et de la réduction des coûts, les entreprises sont tenues d'utiliser des médias de communication efficace du type Internet permettant des échanges de mail, des sites de e-commerce, des edi (échange de documents informatisés).

Les entreprises échangent de plus en plus de documents. Ces documents contiennent de plus en plus informations. Ces informations ont de plus en plus de valeur.

Par ailleurs, les entreprises sont tenues d'aller vite. Elles ne prennent pas toujours toutes les précautions qu'elles devraient prendre.

Troisième facteur de risque : l'ouverture des entreprises sur le monde implique que les systèmes informatiques soient eux aussi de plus en plus ouverts vers l'extérieur. Les systèmes informatiques sont interconnectés. Le LAN de

l'entreprise (Local Area Network. Réseau local de l'entreprise) devient un des postes du réseau mondial.

On constate également que les systèmes informatiques sont de plus en plus complexes. Ils présentent de ce fait des bugs autrement dits trous de sécurité. Par ailleurs des systèmes informatiques complexes sont difficiles à administrer et par conséquent difficiles à sécuriser.

La statistique 2001 du CERT (Computer Emergency Response Team) a répertorié, en 2001, 52658 délits, soit une croissance de 142% par rapport à 2000.

Comment réussit-on à pénétrer un système informatique ?

La quasi-totalité des attaques de vulnérabilité peut être répartie en trois classes :

- (a) Les attaques exploitant une faiblesse des protocoles utilisés (par exemple le Sniffing sur IP). Le Sniffing sur IP est une technique qui consiste à intercepter une communication sur un réseau pour obtenir des informations.
- (b) Les attaques exploitant un bug se situant dans la pile TCP/IP du système d'exploitation. Certaines attaques sont connues sous le nom de « Ping de la mort », « Teardrop ».

On rappelle brièvement qu'au sens de la présente invention les sigles :

- TCP : Transmission Control Protocol, désigne un Protocole de transport (niveau OSI/4) utilisé dans la famille de protocoles TCP/IP,
- TCP/IP : Transmission Control Protocol/Internet Protocol, désigne une famille de protocoles utilisés dans l'interconnexion de réseaux de type IP.

- (c) Les attaques "applicatives" utilisant les données transportées. On peut notamment mentionner des attaques "applicatives" exploitant des bugs dans les applications de communication des systèmes, par exemple des trous de sécurité dans les serveurs DNS bind ou dans les serveurs Web IIS. On

rappelle brièvement qu'au sens de la présente invention les sigles :

- DNS (Domain Name System) désigne un Protocole "applicatif" permettant la conversion de nom de système (par exemple : www.yahoo.com) en adresse IP (par exemple : 123.234.231.135),
- IP (Internet Protocol) désigne un protocole de réseau (Niveau OSI/3) utilisé sur le réseau Internet.

Il ressort des statistiques que la grande majorité des vulnérabilités découvertes se trouvent au niveau des attaques "applicatives". Ainsi, la principale menace se situe au niveau des trous de sécurité des applications de communication.

Tel est le problème posé par la présente invention : réduire les risques des attaques "applicatives".

L'art antérieur

On connaît deux technologies pour résoudre le problème posé et assurer la sécurité des réseaux IP :

La technologie, ci-après dénommée technologie "Stateful",

La technologie, ci-après dénommée technologie "Proxy".

(a) La technologie "Stateful" autrement dit maintien d'une table de connexion active

(a1) La technologie de "filtrage statique de paquet" (static packet filtering)

Les premières fonctionnalités de protection des réseaux IP étaient intégrées dans des routeurs. Les routeurs intègrent un mécanisme de filtrage de paquets IP statiques. En fonction des informations lues dans l'entête des paquets IP, au niveau des entêtes Réseau et Transport, le paquet est accepté ou non grâce à une liste de règles de filtrage définie par un administrateur. L'inconvénient principal de cette technologie est son côté statique. Elle ne peut rattacher un "paquet de réponse" à un "paquet de requête" émis quelques instants plus tôt. Par conséquent, lorsqu'on utilise une technologie de "filtrage statique de paquet", on est obligé d'accepter tous les

"paquets de réponse" sans pouvoir les rattacher aux requêtes précédemment émises. Il en résulte un problème en terme de sécurité puisqu'il suffit, par exemple, de positionner le drapeau ACK dans l'entête TCP d'un paquet pour que ce paquet soit accepté par le routeur. On rappelle brièvement qu'au sens de la présente invention le sigle ACK (ACKnowledgement, Accusé de réception) désigne un drapeau utilisé dans une entête de type TCP.

(a2) La technologie "Stateful"

La technologie "Stateful" surmonte en partie cet inconvénient en gérant une table de connexions actives, qui permet de rattacher les "paquets de réponse" aux "paquets de requête" émis précédemment. De plus, cette technologie implique généralement la lecture d'informations dans les données transportées, par opposition aux informations contenues dans l'en tête du paquet, pour permettre la gestion des connexions secondaires, basées sur des ports dynamiques. Par exemple, tout transfert FTP utilise une connexion secondaire dynamique, dont les ports sont négociés via la connexion de contrôle sur le port tcp/21. On rappelle brièvement qu'au sens de la présente invention le sigle FTP (File Transfer Protocol) désigne un protocole utilisé pour transférer des fichiers sur un réseau de type TCP/IP.

La technologie "Stateful" est généralement implémentée dans le noyau des systèmes, voire embarquée dans un système temps réel, ce qui assure de bonnes performances en termes de débit. En revanche la technologie "Stateful" ne permet pas d'assurer le respect des protocoles "applicatifs" au cours d'un échange de données, puisque la technologie "Stateful" se limite à extraire des données transportées les informations nécessaires à l'établissement et au maintien des connexions secondaires. Or, ainsi que cela a été expliqué, les risques d'attaque se situent principalement au niveau des données transportées.

(b) La technologie "Proxy"

Dans le cas de la technologie "Proxy", autrement appelée technologie "Mandataire", le client ne s'adresse pas directement au serveur. Par exemple, le browser appelé aussi navigateur, se connecte au serveur Web également appelé serveur réseau, en passant par un "Proxy" qui va effectuer la requête à sa place et lui renvoyer la réponse.

Cette technologie permet donc de filtrer les données transportées, ce qui a un intérêt évident en terme de sécurité. Par contre, son implémentation en tant qu'application située "au-dessus" d'un système d'exploitation, la rend beaucoup moins performante en termes de débit que la technologie "Stateful". Cet inconvénient majeur de la technologie "Proxy" entraîne des performances insuffisantes par rapport aux débits recherchés sur les réseaux IP.

Conclusion

On peut donc résumer de la manière suivante les inconvénients des solutions connues.

La sécurité de la technologie "Stateful" est insuffisante.

Le débit de la technologie "Proxy" est insuffisant

La solution selon l'invention

La technologie proposée par la présente invention sera ci-après désignée par le sigle FAST, ou également en langue anglaise : Fast Applicative Shield Technology. La technologie FAST résout le problème posé en évitant les inconvénients des technologies connues "Stateful" et "Proxy ". La technologie FAST permet de sécuriser l'accès aux systèmes d'information en évitant les risques d'attaques "applicatives" et en limitant les pertes de débit.

Procédé

L'invention concerne un procédé pour sécuriser l'accès logique à des informations et/ou à des ressources informatiques d'un ensemble d'équipements informatiques en ralentissant le moins possible l'accès logique. L'ensemble d'équipements informatiques échange des données avec un réseau de

télécommunication informatique, via un dispositif d'accès. Les données comportent des données transportées conformément à au moins un protocole applicatif et des données de transport. Le dispositif d'accès comporte un système d'exploitation.

Le procédé selon l'invention comprend les étapes suivantes :

- l'étape de définir pour chaque protocole applicatif, un automate à état fini,
- l'étape de modéliser, sous la forme d'un modèle, chaque automate à état fini,
- l'étape de générer au moyen d'un interpréteur, à partir de chaque modèle, un module d'analyse de chaque protocole applicatif,
- l'étape de filtrer, dans le système d'exploitation, les données transportées, au moyen des modules d'analyse.

De préférence, selon l'invention, le procédé comprend en outre l'étape de vérifier au moyen des modules d'analyse la conformité des données transportées par rapport aux protocoles applicatifs concernés.

De préférence, selon l'invention, le procédé comprend en outre l'étape de restreindre au moyen du module d'analyse les possibilités offertes par un protocole applicatif.

Grâce à la combinaison de ces deux fonctionnalités (Vérifier et Restreindre), la technologie selon l'invention permet de détecter et de bloquer un nombre important d'attaques "applicatives". Il a pu être établi que ces deux fonctionnalités permettent de détecter et de bloquer 90% des attaques connues sur les serveurs Web Apache et IIS sans qu'il soit nécessaire de leur intégrer une "base de signature d'attaques" comme dans le cas des systèmes de détection d'intrusion.

De préférence, selon l'invention, le procédé comprend en outre l'étape, pour un administrateur réseau, de paramétrer les modules d'analyse en fonction de restrictions prédéterminées.

Dispositif

L'invention concerne également un dispositif d'accès pour sécuriser l'accès logique à des informations et/ou à des ressources informatiques d'un ensemble d'équipements informatiques en ralentissant le moins possible l'accès logique. L'ensemble d'équipements informatiques échange des données avec un réseau de télécommunication informatique, via le dispositif d'accès. Les données comportent des données transportées conformément à au moins un protocole applicatif et des données de transport. Le dispositif d'accès comporte :

- un système d'exploitation comportant un module d'analyse approprié pour chaque protocole applicatif,
- des moyens de filtration pour filtrer, dans le système d'exploitation, les données transportées, au moyen des modules d'analyse.

De préférence, selon l'invention, chaque module d'analyse implémente un automate à états finis représentatif d'un protocole applicatif déterminé.

De préférence, selon l'invention, les modules d'analyse comportent des premiers moyens de traitement informatique pour vérifier la conformité des données transportées par rapport aux protocoles applicatifs concernés.

De préférence, selon l'invention, les modules d'analyse comportent des seconds moyens de traitement informatique pour restreindre les possibilités offertes par un protocole applicatif.

De préférence, selon l'invention, le dispositif d'accès comprend en outre des moyens de paramétrage permettant à un administrateur réseau de paramétrer les modules d'analyse en fonction de restrictions prédéterminées.

Description détaillée

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de variantes de réalisation de l'invention données à titre d'exemple indicatif et non limitatif, et de la

- figure 1 qui représente de manière schématique un réseau local d'entreprise 3 protégé par un dispositif 6 selon l'invention contre des attaques provenant d'un réseau de communication informatique de type Internet,
- figure 2 qui représente la structure des données 4 échangées via un dispositif 6 selon l'invention,
- figure 3 qui représente de manière schématique un dispositif 6 selon l'invention,
- figure 4 qui représente de manière schématique la méthode de construction d'un module d'analyse 14 à partir d'un automate à états finis.

On va maintenant décrire en se référant aux figures et notamment à la figure 1 un réseau local d'entreprise 3 protégé par un dispositif 6 selon l'invention contre des attaques provenant d'un réseau de communication informatique 5 de type Internet.

Le dispositif d'accès 6 a pour objet de sécuriser l'accès logique à des informations 1 et/ou à des ressources informatiques 2 d'un ensemble d'équipements informatiques 3 en ralentissant le moins possible ledit accès logique.

L'ensemble d'équipements informatiques 3 échange des données 4 avec un réseau de télécommunication informatique 5, via ledit dispositif d'accès 6. Dans le cas de la variante de réalisation décrite le réseau de télécommunication informatique 5 est du type Internet. Les équipements informatiques 3 peuvent être des serveurs, des postes de travail etc ….

De manière connue en soi, les données 4 comportent des données transportées 7 conformément à au moins un protocole applicatif 8 et des données de transport 9 (voir figure 2).

Le dispositif d'accès 6 selon l'invention comprend un système d'exploitation 10. Le système d'exploitation 10 comporte des modules d'analyse 14 appropriés pour chaque protocole applicatif 8 utilisé. Les modules d'analyse 14 du système d'exploitation 10 filtrent les données transportées 7.

Chaque module d'analyse 14 implémente un automate à états finis 11 représentatif d'un protocole applicatif 8 déterminé. Pour réaliser un module d'analyse 14, on modélise sous la forme d'un modèle 12 chaque automate à états finis 11, notamment en utilisant une matrice de transition des états. Puis on génère au moyen d'un interpréteur 13, à partir de chaque modèle 12, le module d'analyse 14 de chaque protocole applicatif 8 (voir figure 4).

Chaque module d'analyse 14 comporte des premiers moyens de traitement informatique 17 pour vérifier la conformité des données transportées 7 par rapport aux protocoles applicatifs 8 concernés. Chaque module d'analyse 14 comporte en outre des seconds moyens de traitement informatique 18 pour restreindre les possibilités offertes par un protocole applicatif 8.

Le système d'exploitation et les modules d'analyse 14 associés constituent des moyens de filtration des données transportées 7.

Le dispositif d'accès 6 comprend en outre des moyens de paramétrage 19. Ces moyens de paramétrage 19 permettent à un administrateur réseau 15 de paramétrer les modules d'analyse 14 en fonction de restrictions prédéterminées 16, ainsi que cela sera ci-après précisé.

Grâce au dispositif d'accès 6 selon l'invention, il est possible de vérifier le bon respect des protocoles applicatifs, ce qui permet de bloquer un très grand nombre d'attaques "applicatives" sans les connaître, notamment celles violant les RFC ("Normes IP "). On rappelle brièvement qu'au sens de la présente invention le sigle RFC (Request For Comment) désigne différents documents normatifs dans lesquels sont spécifiés les différents protocoles de la famille TCP/IP.

De plus, la technologie selon l'invention permet de restreindre les possibilités offertes par une application. Par exemple, la technologie selon l'invention permet de limiter les

commandes disponibles sur un protocole "applicatif" ou de n'autoriser l'accès qu'à certaines données, etc...

Grâce à la combinaison de ces deux fonctionnalités (Vérifier et Restreindre), la technologie selon l'invention permet de détecter et de bloquer un nombre important d'attaques "applicatives". Il a pu être établi que ces deux fonctionnalités permettent de détecter et de bloquer 90% des attaques connues sur les serveurs Web Apache et IIS sans qu'il soit nécessaire de leur intégrer une "base de signature d'attaques" comme dans le cas des systèmes de détection d'intrusion.

La technologie selon l'invention a été développée sur un système d'exploitation Linux. Il est à la portée de l'homme de métier de la mettre œuvre sur d'autres systèmes du même type.

NOMENCLATURE

Groupe nominal	Réf. Num.
informations	1
ressources informatiques	2
ensemble d'équipements informatiques	3
données	4
réseau de télécommunication informatique	5
dispositif d'accès	6
données transportées	7
protocole applicatif	8
données de transport	9
système d'exploitation	10
automate à états finis	11
modèle	12
interpréteur	13
module d'analyse	14
administrateur réseau	15
restrictions prédéterminées	16
premiers moyens de traitement informatique	17
seconds moyens de traitement informatique	18
moyens de paramétrage	19

REVENDICATIONS

1. Procédé pour sécuriser l'accès logique à des informations (1) et/ou à des ressources informatiques (2) d'un ensemble d'équipements informatiques (3) en ralentissant le moins possible ledit accès logique ;

ledit ensemble d'équipements informatiques (3) échangeant des données (4) avec un réseau de télécommunication informatique (5), via un dispositif d'accès (6) ;

lesdites données (4) comportant des données transportées (7) conformément à au moins un protocole applicatif (8) et des données de transport (9) ;

ledit dispositif d'accès (6) comportant un système d'exploitation (10) ;

ledit procédé comprenant les étapes suivantes :

- l'étape de définir pour chaque protocole applicatif (8), un automate à états finis (11),
- l'étape de modéliser, sous la forme d'un modèle (12), chaque automate à états finis (11),
- l'étape de générer au moyen d'un interpréteur (13), à partir de chaque modèle (12), un module d'analyse (14) de chaque protocole applicatif (8),
- l'étape de filtrer, dans ledit système d'exploitation (10), lesdites données transportées (7), au moyen desdits modules d'analyse (14).

2. Procédé selon la revendication 1 ; ledit procédé comprenant en outre :

- l'étape de vérifier au moyen desdits modules d'analyse (14) la conformité desdites données transportées (7) par rapport auxdits protocoles applicatifs (8) concernés.

3. Procédé selon l'une quelconque des revendications 1 ou 2 ; ledit procédé comprenant en outre :

- l'étape de restreindre au moyen dudit module d'analyse (14) les possibilités offertes par un protocole applicatif (8).

4. Procédé selon la revendication 3 ; ledit procédé comprenant en outre :

- l'étape, pour un administrateur réseau (15), de paramétrer lesdits modules d'analyse (14) en fonction de restrictions prédéterminées (16).

Dispositif

5. Dispositif d'accès (6) pour sécuriser l'accès logique à des informations (1) et/ou à des ressources informatiques (2) d'un ensemble d'équipements informatiques (3) en ralentissant le moins possible ledit accès logique ;

ledit ensemble d'équipements informatiques (3) échangeant des données (4) avec un réseau de télécommunication informatique (5), via ledit dispositif d'accès (6) ;

lesdites données (4) comportant des données transportées (7) conformément à au moins un protocole applicatif (8) et des données de transport (9) ;

ledit dispositif d'accès (6) comportant:

- un système d'exploitation (10) comportant un module d'analyse (14) approprié pour chaque protocole applicatif (8),

- des moyens de filtration pour filtrer, dans ledit système d'exploitation (10), lesdites données transportées (7), au moyen desdits modules d'analyse (14).

6. Dispositif d'accès (6) selon la revendication 5 ; chaque module d'analyse (14) implémentant un automate à états finis (11) représentatif d'un protocole applicatif (8) déterminé.

7. Dispositif d'accès (6) selon l'une quelconque des revendications 5 ou 6 ; lesdits modules d'analyse (14) comportant :

- des premiers moyens de traitement informatique (17) pour vérifier la conformité desdites données transportées (7) par rapport auxdits protocoles applicatifs (8) concernés.

8. Dispositif d'accès (6) selon l'une quelconque des revendications 5 à 7 ; lesdits modules d'analyse (14) comportant :

- des seconds moyens de traitement informatique (18) pour restreindre les possibilités offertes par un protocole applicatif (8).

9. Dispositif d'accès (6) selon la revendication 8 ; ledit dispositif d'accès (6) comprenant en outre :

- des moyens de paramétrage (19) permettant à un administrateur réseau (15) de paramétrer lesdits modules d'analyse (14) en fonction de restrictions prédéterminées (16).

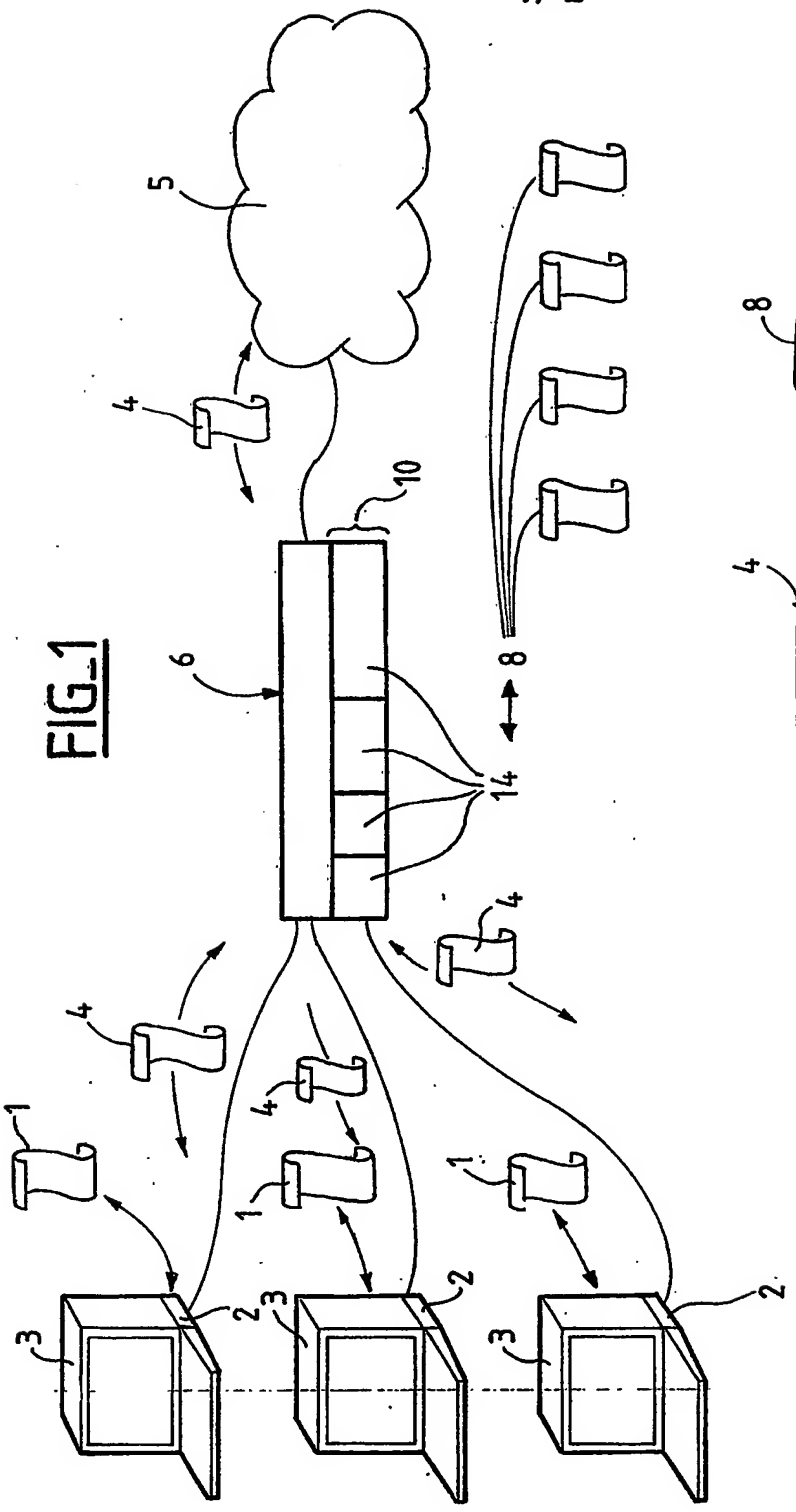

FIG_1

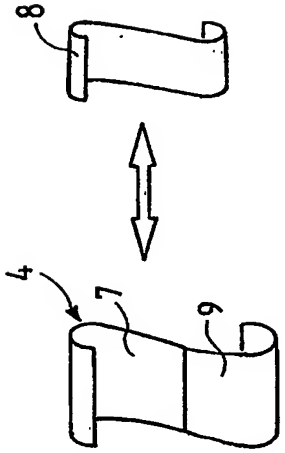

FIG_2

FIG_3

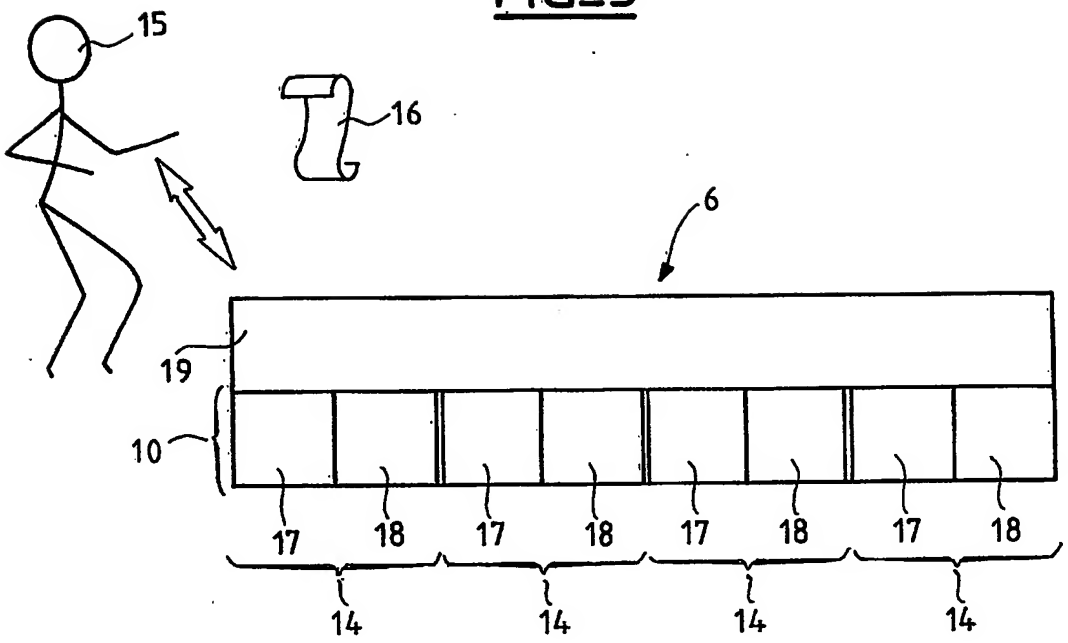

FIG_4